UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,444	07/05/2001	Elsie Van Herreweghen	CH920000009US1	4090

7590 01/12/2007

Steven Fischman, Esq
SULLY SCOTT MURPHY & PRESSER
400 Garden City Plaza
Suite 300
Garden City, NY 11530-3319

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/899,444	HERREWEGHEN, ELSIE VAN	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28 and 30-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28 and 30-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response the amendment filed on November 15, 2006.

2. Claims 1-28 and 30-35 are pending.

3. The 112/1st paragraph rejection to claims 1-28 and 30-35 are withdrawn as the amendment overcomes the 112/1st paragraph rejections.

Response to Arguments

4. Applicant's arguments with respect to amended claims 1-28 and 30-35 have been considered but are not persuasive. Applicant's arguments are insufficient for two reasons: First, the substantive portion of the arguments by the applicant (Remarks, pg. 12, last paragraph-pg. 13, paragraph 5) only distinguish the references individually from the claimed invention: one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Second, applicant's allegation that the combination of the prior art does not disclose the claimed invention (Remarks, pg. 13, paragraph 6) is merely a bald assertion without providing a rational why this is so. Hence, as outlined below, the 103 rejections that the claimed invention is rendered obvious by the teachings of Lewis, Ellison, and/or Muftic, and/or Brands are maintained.

Claim Objections

5. Claim 16 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 16 defines the limitation wherein the first private signature key is identical to the second private signature key. However, this feature contradicts the limitation in parent claim 13, that the second private-public signature pair is different than the first private-public signature key pair.

Claim Rejections - 35 USC § 103

6. Claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35 are rejected under 35 U.S.C. 102(e) as being unpatentable over Lewis et al. U.S. Patent No. 6,233,565 (hereinafter Lewis) in view of Ellison et al. USPN 6,976,162 (hereinafter Ellison) and Brand USPN 5,604,805 (hereinafter Brand).

7. As per claim 6, Lewis discloses a receipt generation method, comprising generating an electronic receipt in a communication system providing a public key encryption system, including the steps of:

a. receiving a message from a sender, the message is electronically signed by the sender using a private signature key owned by the sender, whereby the message includes a transaction request and a reference to a designated owner

of a receipt to be generated (Lewis, col. 4:20-27; cols. 7 and 8, TABLE 1, "Transaction Type");

b. authenticating the message using a public signature verification key associated to the private signature key held by the sender of the message (Lewis, 4:24-27; cols. 7 and 8: TABLE 1 under "Transaction Type": "authentication client 2n to server", under "Transaction Server 190" and "Master Server 300");

c. issuing a receipt including the reference to the designated owner of the receipt and details for what the receipt has been given to provide the designated owner with the receipt (Lewis, 4:32-38); and

d. electronically signing the receipt with the public signature key assigned to an issuer issuing the receipt (Lewis, 4:41-44).

8. Lewis does not teach using a pseudonym on the message from the sender, wherein the pseudonym is issued using a first private-public key pair, and the receipt enables the owner to verify ownership of the receipt while maintaining the owner anonymous or pseudonymous. Ellison discloses producing pseudonyms by generating a key pair and certifying the generated public key by a trusted center to withhold the identity of a user in transactions requiring the use of the pseudonym key to certify digital signatures of the user (Ellison, col. 3:8-13; 3:57-5:9). In the method of Lewis, the public/private keys used to sign and verify the signatures of the receipts are rendered anonymous using the anonymous keys as taught by Ellison. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to verify

ownership of the receipt while maintaining the anonymity of the owner of the receipt, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, 1:65-2:1).

9. Finally, Lewis does not disclose using a second private-public signature key pair different than the first private-public signature key pair to verify the ownership of the receipt. Brand discloses a cryptographic concept of using different pseudonyms at different organizations such that the pseudonyms are unlinkable. (col. 2:15-34) This concept as applied to the teachings of Lewis and Ellison suggest using different pseudonym key pairs for different types of transactions to ensure unlinkablity of the transaction between the user and the organization issuing the receipt, and the transaction between the user and the organization verifying the receipt. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a second private-public signature key pair different than the first private-public signature key pair to verify the ownership of the receipt, while maintaining the owner anonymous or pseudonymous. This would ensure better privacy for the user since the organization generating the receipt and the organization validating the ownership of the receipt are not able to collude to identify the owner of the receipt, Brand, ibid. The aforementioned cover the limitations of claim 6.

10. As per claim 7, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the method further includes the steps of performing the requested transaction, and returning the receipt to the sender (Lewis, col. 4:32-33).

11. As per claims 8-10, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Ellison discloses using a pseudonym for communicating and using a pseudonym as a reference to a designated owner (Ellison, col. 1:65-2:1; Abstract). It would be obvious to one of ordinary skill in the art at the time the invention was made to use a pseudonym for communication and designating the owner with a pseudonym to be used as a reference to the owner since it is desirous to maintain the privacy of a user transferring certified information (Ellison, ibid). Further, an anonymous communication connection is necessarily required in a pseudonym protocol. The aforementioned cover the limitations of claims 8-10.

12. As per claim 11, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the designated owner of the receipt is the sender (Lewis, col. 4:32-35).

13. As per claim 13, the rejections of claims 7 and 11 under 35 U.S.C. 103(a) are incorporated herein. In addition, the method disclosed by Lewis is also a method of proving ownership of a receipt (holder of the digital receipt signed by both the owner and the issuer proves ownership of the receipt) including the steps of:

e. a user using a pseudonym to create a first message including a transaction request and a reference to a designated owner of a receipt to be generated in response to receiving the message, wherein the pseudonym is

issued to the user using a first private-public signature key pair (Lewis, col. 4:20-27; the sender of the transaction request is the designated owner of the receipt; Ellison, 4:10-14);

f. the user electronically signing the message using the first private signature key (Lewis, 4:24-25; cols. 7 and 8: TABLE 1 under "Transaction Type": "authentication client 2n to server");

g. sending the first message to a first addressee (Lewis, 4:20-27; first addressee is the transaction server; and

h. receiving the receipt from the first addressee, the receipt being electronically signed by the first addressee using a second private signature key of a second private-public key pair assigned to the first addressee, wherein the receipt includes information as for what the receipt has been issued and the reference to the designated owner of the receipt and thereby to enable the owner to verify ownership of the receipt by using the second private-public signature key pair different then the first private-public signature key pair while maintaining the owner anonymous or pseudonymous (Lewis, 4:32-43 [the receipt comprises the client digital signature and the server digital signature, which generated the receipt]; Ellison, 3:8-13; 3:57-5:9 [digital signature created by pseudonym public key]).

14. It would be obvious to one of ordinary skill in the art at the time the invention was made to maintain the anonymity of the owner, since it is desirous to maintain the privacy

of a user transferring certified information (Ellison, col. 65-2:1). The aforementioned cover the limitations of claim 13.

15. As per claim 17, the rejection of claim 13 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the reference to the designated owner of the receipt is a pseudonym used by the owner of the receipt (Lewis, 4:32-34 [the receipt comprises the client's digital signature]; Ellison, col. 3:8-13; 3:57-5:9 9 [digital signature created by pseudonym public key]). It would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the designated owner of the receipt to be a pseudonym used by the owner of the receipt, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, col. 1:65-2:1). The aforementioned cover the limitation of claim 17.

16. As per claim 19, the rejection of claim 13 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the designated owner of the receipt is identical to a sender sending the first message to the first addressee (Lewis, col. 4, 20-27 [the sender of the transaction request is the designated owner of the receipt]).

17. As per claim 20, the rejections of claims 13 and 19 under 35 U.S.C. 103(a) are incorporated herein. In addition, the method further comprises creating a second message including the receipt; electronically signing the second message using a

second private signature key; and sending the second message to the designated owner of the receipt (Lewis, col. 4:32-43).

18. As per claims 21 and 22, the rejection of claim 20 under 35 U.S.C. 103(a) is incorporated herein. In addition, Ellison discloses using pseudonyms to withhold the identity of a user in transactions requiring the use of certifying a signature, wherein the signature remains anonymous (col. 3:8-13; 3:57-5:9). It would be obvious to one of ordinary skill in the art at the time the invention was made wherein the sending and receiving of the first and second messages are performed by using a pseudonym, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, 1:65-2:1). Finally, an anonymous communication connection is necessarily required in a pseudonym protocol. The aforementioned cover the limitations of claims 21 and 22.

19. As per claims 25 and 26, they are apparatus claims corresponding to claims 6 and 13, and they do not teach or define above the information claimed in claims 6 and 13. Therefore, claims 25 and 26 are rejected as being unpatentable over Lewis in view of Ellison and Brand for the same reasons set forth in the rejections of claims 6 and 13.

20. As per claims 27, 28, 31 and 32, the rejections of claims 6 and 13 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to perform the methods of claims 6 and 13 are embodied in a program of instructions executable by a machine (Lewis, Figure 2).

21. As per claims 34 and 35, the rejections of claims 6, 13, 25, 26, 27, 28, 31 and 32 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to affect the functions of the devices of claims 25 and 26 comprise computer readable program (Lewis, col. 2:10-14).

22. Claims 1-5, 23, 24, 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Muftic U.S. Patent No. 5,850,442 (hereinafter Muftic) and Ellison.

23. As per claims 1-4, Lewis discloses a method comprising generating an electronic receipt in a communication system providing a public key encryption infrastructure, wherein a server generation module in response to an electronic payment transaction, generates a receipt and transmits the receipt, wherein the receipt comprises a client digital signature and a server digital signature, and a data set uniquely identifying the executed transaction, wherein the receipt authenticates the electronic transaction, and the receipt includes details for what the receipt has been given and a reference to a designated owner (Lewis, col. 4:24-44). Lewis does not expressly teach how the electronic receipt is authenticated. Muftic teaches an ordinary means of authenticating a signed message by a sender of the message using a public key encryption infrastructure including the following steps:

i. receiving a message from a sender, the message being electronically signed by the sender using a private signature key owned by the sender; the corresponding public key of the sender is provided within a digital certificate by a trusted issuer and signed by the issuer having given the certificate, wherein the certificate includes details for the context of the certificate and a reference to the owner of the certificate (Muftic, col. 2:42-51; 3:35-52; 4:27-32; digital certificates in the standard X.509 define attributes including certificate context and key subscriber identity values);

j. obtaining a public signature verification key on the basis of the reference to the owner of the certificate (digital certificates enables trusted retrieval of the public signature verification key); and

k. examining whether or not the private signature key used for electronically signing the message is associated to the public signature verification key obtained on the basis of the reference to the owner of the certificate (Muftic, 2:44-51).

24. Although Muftic does not expressly teach submitting the certificate holding the public signature verification key and signed by the issuer with the original signed message, the step of including the certificate with the signed message is a trivial combination since proper verification of the signed message requires the signed certificate (see Muftic, 3:30-33); moreover, the combination of disparate parts has been found to be an obvious feature. See In re Larson 144 USPQ 347 (CCPA 1965). Further, the digital certificate taught by Muftic is operatively equivalent to the electronic

receipt: both maintain a record of an agreement/transaction between the owner and the issuer. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to verify the receipt according to the recited steps of applicant's claim 1, since it is desirous to cryptographically verify the receipt as being owned by the sender and issued by the issuer (Lewis, 4:36-38; Muftic, 2:10-14 and 3:47-49).

25. Finally, Lewis does not teach the reference to the owner of the receipt is a pseudonym used by the owner of the receipt, wherein a certificate securely links the pseudonym to the public signature verification key, such that verification of ownership of the receipt is enabled while maintaining the owner anonymous or pseudonymous. Ellison discloses creating user pseudonyms by generating a key pair and certifying the generated public key by a trusted center to withhold the identity of a user in transactions requiring the use of the pseudonym key to certify digital signatures of the user, (Ellison, col. 3:8-13; 3:57-5:9). In the method of Lewis, the keys used to sign and to verify the signatures of the receipts are rendered anonymous using the anonymous keys as taught by Ellison. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the owner of the receipt to be a pseudonym used by the owner of the receipt and a certificate to securely link the pseudonym to the public signature verification key, such that verification of ownership of the receipt is enabled while maintaining the owner anonymous or pseudonymous, since it is desirous to maintain the privacy of a user transferring certified information (Ellison, 1:65-2:1). The aforementioned cover the limitations of claims 1-4.

26. As per claim 5, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the method further comprises the step of authenticating the receipt using a public signature verification key assigned to the issuer of the receipt (Lewis, col. 4:24-44; Muftic, col. 3:44-52).

27. As per claim 24, it is an apparatus claims corresponding to claim 1, and it does not teach or define above the information claimed in claim 1. Therefore, claim 24 is rejected as being unpatentable over Lewis in view of Muftic and Ellison for the same reasons set forth in the rejection of claim 1.

28. As per claims 23 and 30, the rejections of claims 1 and 24 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to perform the method of claim 1 is embodied in a program of instructions executable by a machine (Lewis, Figure 2).

29. As per claim 33, the rejections of claims 1, 23, 24 and 30 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, means to affect the functions of the device of claim 24 comprise a computer readable program (Lewis, col. 2:10-14).

30. Claims 12, 14-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Ellison, Brand and Muftic.

31. As per claim 12, the rejection of claim 6 under 35 U.S.C. 103(a) is incorporated herein. (supra) Lewis does not expressly disclose the reference to a designated owner is a public signature key associated to a private signature verification key held by the designated owner of the receipt. (Lewis discloses the receipt comprises a client digital signature and a data set uniquely identifying the executed transaction) However, a public signature key as the reference to a designated owner is an obvious enhancement because it uniquely identifies the corresponding private signature key used to sign the receipt. As disclosed by Muftic, public keys are conventionally certified by means of a certificate to associate a signature key with a subscriber (col. 2:42-51; 3:35-52; 4:27-32). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to a designated owner to be a public signature key associated to a private signature verification key held by the designated owner of the receipt, because it enables a certified reference to the signed receipt. The aforementioned cover the limitations of claim 12.

32. Regarding claims 14, 15 and 18, the rejection of claim 13 under 35 U.S.C. 103(a) is incorporated herein. (supra) Lewis does not expressly teach creating a second message including the receipt to authenticate the receipt. Muftic teaches an ordinary means of authenticating a signed message by a sender of the message using a public key encryption infrastructure including the following steps:

I. receiving a message from a sender, the message being electronically signed by the sender using a private signature key owned by the sender; the

corresponding public key of the sender is provided within a digital certificate by a trusted issuer and signed by the issuer having given the certificate, wherein the certificate includes details for the context of the certificate and a reference to the owner of the certificate (Muftic, col. 2:42-51; 3:35-52; 4:27-32; digital certificates in the standard X.509 define attributes including certificate context and key subscriber identity values);

m. obtaining a public signature verification key on the basis of the reference to the owner of the certificate (digital certificates enables trusted retrieval of the public signature verification key); and

n. examining whether or not the private signature key used for electronically signing the message is associated to the public signature verification key obtained on the basis of the reference to the owner of the certificate (Muftic, 2:44-51).

33. Although Muftic does not expressly teach submitting the certificate holding the public signature verification key and signed by the issuer with the original signed message, the step of including the certificate with the signed message is a trivial combination since proper verification of the signed message requires the signed certificate (see Muftic, 3:30-33); moreover, the combination of disparate parts has been found to be an obvious feature. See In re Larson 144 USPQ 347 (CCPA 1965). Further, the digital certificate taught by Muftic is operatively equivalent to the electronic receipt: both maintain a record of an agreement/transaction between the owner and the issuer. Hence, it would be obvious to one of ordinary skill in the art at the time the

invention was made to verify the receipt according to the recited steps of applicant's claim 14 and 18, since it is desirous to cryptographically verify the receipt as being owned by the sender and issued by the issuer (Lewis, 4:36-38; Muftic, 2:10-14 and 3:47-49). Finally, the user signs the first and second messages using their private signature key, hence, the first private signature key is identical to the second private signature key. The aforementioned cover the limitations of claims 14, 16 and 18.

34. As per claim 15, the rejection of claim 14 under 35 U.S.C. 103(a) is incorporated herein. (supra) Lewis does not expressly teach the first addressee is identical to the second addressee. However, it is notoriously well known for certification parties who issue certificates also verify the certificates. For example, trusted certification issuers such as VeriSign both issue certificates and verify issued certificates. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first addressee to be identical to the second addressee since a single party may be best equipped to handle both roles as known to one of ordinary skill in the art. Furthermore, it is desirable for a server issuing a receipt to be able to validate the receipt, since a receipt acts as a record of services requested and paid for by the user. The aforementioned cover the limitations of claim 15.

Conclusion

35. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jk
January 4, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100